

4.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Helena HANDSCHUH

Application No.: 09/774,674

Filed: February 1, 2001

For: COUNTERMEASURE METHOD IN AN)
ELECTRONIC COMPONENT USING A)
PUBLIC KEY CRYPTOGRAPHY)
ALGORITHM ON AN ELLIPTIC)
CURVE)



Group Art Unit: 2131

Examiner: Unassigned

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior application in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed:

French Patent Application No. 0007109

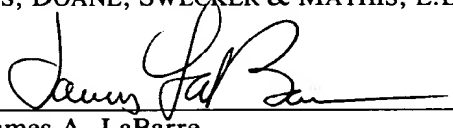
Filed: June 2, 2000.

In support of this claim, enclosed is a certified copy of the prior foreign application. This application is referred to in the oath or declaration. Acknowledgment of receipt of this certified copy is requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: June 29, 2001

By: 
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

THIS PAGE BLANK (USPTO)



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le **15 FEV. 2001**

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30
<http://www.inpi.fr>

THIS PAGE BLANK (USPTO)



26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

08 540 W / 260899

2 JUIN 2006 REMISSÉ DES FICHS DATE 13 INPI MARSEILLE LIEU N° D'ENREGISTREMENT 0007109 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE 02 JUIN 2006 PAR L'INPI		1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE GEMPLUS Parc d'activités de GEMENOS Avenue du Pic de Bertagne 13881 GEMENOS FRANCE	
Vos références pour ce dossier (facultatif) GEM 893			
Confirmation d'un dépôt par télécopie <input type="checkbox"/> N° attribué par l'INPI à la télécopie			
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
Demande de brevet initiale		N° _____ Date ____/____/____	
ou demande de certificat d'utilité initiale		N° _____ Date ____/____/____	
Transformation d'une demande de brevet européen		<input type="checkbox"/> N° _____ Date ____/____/____	
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) PROCÉDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE SUR COURBE ELLIPTIQUE			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation _____ N° _____ Date ____/____/____ Pays ou organisation _____ N° _____ Date ____/____/____ Pays ou organisation _____ N° _____ <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR		<input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»	
Nom ou dénomination sociale		GEMPLUS	
Prénoms			
Forme juridique		S.A	
N° SIREN		3 9 0 0 4 9 0 7 0	
Code APE-NAF		7 4 8 D	
Adresse	Rue	Parc d'activités de GEMENOS Avenue du Pic de Bertagne	
	Code postal et ville	13881	GEMENOS
Pays		FRANCE	
Nationalité		FRANCE	
N° de téléphone (facultatif)		04 42 36 53 50	
N° de télécopie (facultatif)		04 42 36 63 43	
Adresse électronique (facultatif)		alisee.couteau@gemplus.com	

**BREVET D'INVENTION
CERTIFICAT D'UTILITÉ**

REQUÊTE EN DÉLIVRANCE 2/2

REMISE DES PIÈCES DATE 13 JUIN 2009 LIEU INPI MARSEILLE N° D'ENREGISTREMENT 0007109 NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI	
Vos références pour ce dossier : <i>(facultatif)</i>		GEM 893	
6 MANDATAIRE			
Nom		NONNENMACHER	
Prénom		Bernard	
Cabinet ou Société		GEMPLUS	
N° de pouvoir permanent et/ou de lien contractuel		PG06339 - PG8556	
Adresse	Rue	Parc d'Activités de GEMENOS Avenue du Pic de Bertagne	
	Code postal et ville	13881	GEMENOS
N° de téléphone <i>(facultatif)</i>		04 42 36 53 50	
N° de télécopie <i>(facultatif)</i>		04 42 36 63 43	
Adresse électronique <i>(facultatif)</i>			
7 INVENTEUR (S)			
Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée	
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paiement échelonné de la redevance		Paiement en deux versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non	
RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Requête antérieurement à ce dépôt (joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence):	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		1	
10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) Pierre BRUYERE Ingénieur Brevets		VISA DE LA PRÉFECTURE OU DE L'INPI	

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 1.. / 1..
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

Vos références pour ce dossier (facultatif)		GEM 893	
N° D'ENREGISTREMENT NATIONAL		000 7109	
TITRE DE L'INVENTION (200 caractères ou espaces maximum) PROCÉDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN ŒUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE SUR COURBE ELLIPTIQUE			
LE(S) DEMANDEUR(S) : GEMPLUS Société Anonyme Parc d'Activités de GEMENOS Avenue du Pic de Bertagne 13881 GEMENOS			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		HANDSCHUH	
Prénoms		Hélène	
Adresse	Rue	6 rue de Bigorre	
	Code postal et ville	75014	PARIS
Société d'appartenance (facultatif)		GEMPLUS	
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		Pierre BRUYERE Ingénieur Brevets	

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

THIS PAGE BLANK (USPTO)

**PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT
ELECTRONIQUE METTANT EN ŒUVRE UN ALGORITHME DE
CRYPTOGRAPHIE A CLE PUBLIQUE SUR COURBE ELLIPTIQUE**

La présente invention concerne un nouveau procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de chiffrement à clé publique sur courbe elliptique.

5 Dans le modèle classique de la cryptographie à clef secrète, deux personnes désirant communiquer par l'intermédiaire d'un canal non sécurisé doivent au préalable se mettre d'accord sur une clé secrète de chiffrement K. La fonction de chiffrement et la
10 fonction de déchiffrement utilisent la même clef K. L'inconvénient du système de chiffrement à clé secrète est que ledit système requiert la communication préalable de la clé K entre les deux personnes par l'intermédiaire d'un canal sécurisé,
15 avant qu'un quelconque message chiffré ne soit envoyé à travers le canal non sécurisé. Dans la pratique, il est généralement difficile de trouver un canal de communication parfaitement sécurisé, surtout si la distance séparant les deux personnes est importante.
20 On entend par canal sécurisé un canal pour lequel il est impossible de connaître ou de modifier les informations qui transitent par ledit canal. Un tel canal sécurisé peut être réalisé par un câble reliant deux terminaux, possédés par les deux dites
25 personnes.

Le concept de cryptographie à clef publique fut inventé par Whitfield DIFFIE et Martin HELLMAN en 1976. La cryptographie à clef publique permet de résoudre le problème de la distribution des clefs à
30 travers un canal non sécurisé. Le principe de la cryptographie à clef publique consiste à utiliser une paire de clefs, par exemple une clef publique de chiffrement et une clef privée de déchiffrement. Il

doit être calculatoirement infaisable de trouver la
 clef privée de déchiffrement à partir de la clef
 publique de chiffrement. Une personne A désirant
 communiquer une information à une personne B utilise
 5 la clef publique de chiffrement de la personne B.
 Seule la personne B possède la clef privée associée à
 sa clef publique. Seule la personne B est donc
 capable de déchiffrer le message qui lui est adressé.

Un autre avantage de la cryptographie à clé
 10 publique sur la cryptographie à clé secrète est que
 la cryptographie à clef publique permet
 l'authentification d'un document ou d'une personne ou
 de la provenance d'un document grâce à l'utilisation
 de signatures numériques.

15 La première réalisation de schéma de chiffrement à
 clef publique fut mise au point en 1977 par Rivest,
 Shamir et Adleman, qui ont inventé le système de
 chiffrement RSA. La sécurité de RSA repose sur la
 difficulté de factoriser un grand nombre qui est le
 20 produit de deux nombres premiers. Depuis, de nombreux
 systèmes de chiffrement à clef publique ont été
 proposés, dont la sécurité repose sur différents
 problèmes calculatoires : (cette liste n'est pas
 exhaustive).

25 - Sac à dos de Merckle-Hellman :

Ce système de chiffrement est basé sur la
 difficulté du problème de la somme de sous-
 ensembles.

- McEliece :

30 Ce système de chiffrement est basé sur la
 théorie des codes algébriques. Il est basé sur le
 problème du décodage de codes linéaires.

- ElGamal :

35 Ce système de chiffrement est basé sur la
 difficulté du logarithme discret dans un corps
 fini.

- Courbes elliptiques :

Le système de chiffrement à courbe elliptique constitue une modification de systèmes cryptographiques existants pour les appliquer au domaine des courbes elliptiques.

5 L'utilisation de courbes elliptiques dans des systèmes cryptographiques fut proposé indépendamment par Victor Miller et Neal Koblitz en 1985. Les applications réelles des courbes elliptiques ont été envisagées au début des années 1990. L'avantage de
10 cryptosystèmes à base de courbe elliptique est qu'ils fournissent une sécurité équivalente aux autres cryptosystèmes mais avec des tailles de clef moindres. Ce gain en taille de clé implique une diminution des besoins en mémoire et une réduction
15 des temps de calcul, ce qui rend l'utilisation des courbes elliptiques particulièrement adaptées pour des applications de type carte à puce.

Une courbe elliptique sur un corps fini $GF(q^n)$ (q étant un nombre premier et n un entier) est
20 l'ensemble des points (x,y) avec x l'abscisse et y l'ordonnée appartenant à $GF(q^n)$ ayant pour équation :

$$y^2 = x^3 + ax + b$$

25 si q est supérieur ou égal à 3 et

$$y^2 + x*y = x^3 + a*x^2 + b$$

si $q=2$.

Les deux classes de courbes elliptiques les plus utilisées en cryptographie sont les classes
30 suivantes :

1) Courbes définies sur le corps fini $GF(p)$ (ensemble des entiers modulo p , p étant un nombre premier) ayant pour équation:

$$y^2 = x^3 + ax + b$$

35 2) Courbes élliptiques sur le corps fini $GF(2^n)$ ayant pour équation $y^2 + xy = x^3 + ax^2 + b$

Pour chacune de ces deux classes de courbes, on définit une opération d'addition de points: étant

donné deux points P et Q , la somme $R=P+Q$ est un point de la courbe, dont les coordonnées s'expriment à l'aide des coordonnées des points P et Q suivant des formules dont l'expression est donnée dans l'ouvrage
 5 « Elliptic Curve public key cryptosystem » par Alfred J. Menezes.

Cette opération d'addition permet de définir une opération de multiplication scalaire: étant donné un point P appartenant à une courbe elliptique et un
 10 entier d , le résultat de la multiplication scalaire de P par un point d tel que $Q=d.P=P+P+ \dots +P$ d fois.

La sécurité des algorithmes de cryptographie sur courbes elliptiques est basée sur la difficulté du logarithme discret sur courbes elliptiques, ledit
 15 problème consistant à partir de deux points Q et P appartenant à une courbe elliptique E , de trouver, s'il existe, un entier x tel que $Q=x.P$

Il existe de nombreux algorithmes cryptographiques basés sur le problème du logarithme discret. Ces algorithmes sont facilement
 20 transposables aux courbes elliptiques. Ainsi, il est possible de mettre en oeuvre des algorithmes assurant l'authentification, la confidentialité, le contrôle d'intégrité et l'échange de clé.

Un point commun à la plupart des algorithmes cryptographiques basés sur les courbes elliptiques est qu'ils comprennent comme paramètre une courbe elliptique définie sur un corps fini et un point P appartenant à cette courbe elliptique. La clé privée
 30 est un entier d choisi aléatoirement. La clef publique est un point de la courbe Q tel que $Q=d.P$. Ces algorithmes cryptographiques font généralement intervenir une multiplication scalaire dans le calcul d'un point $R=d.T$ où d est la clef secrète.

35 Dans ce paragraphe, on décrit un algorithme de chiffrement à base de courbe elliptique. Ce schéma est analogue au schéma de chiffrement d'El Gamal. Un message m est chiffré de la manière suivante :

Le chiffreur choisit un entier k aléatoirement et calcule les points $k.P=(x_1,y_1)$ et $k.Q=(x_2,y_2)$ de la courbe, et l'entier $c= x_2 + m$. Le chiffré de m est le triplet (x_1,y_1,c) .

5 Le déchiffreur qui possède d déchiffre m en calculant :

$$(x'_2,y'_2)=d(x_1,y_1) \text{ et } m=c-x'_2$$

Pour réaliser les multiplications scalaires nécessaires dans les procédés de calcul décrits
10 précédemment, plusieurs algorithmes existent :

Algorithme « double and add » ;

Algorithme « addition-soustraction »

Algorithme avec chaînes d'addition ;

Algorithme avec fenêtre ;

15 Algorithme avec représentation signée ;

Cette liste n'est pas exhaustive. L'algorithme le plus simple et le plus utilisé est l'algorithme « double and add ». L'algorithme « double and add » prend en entrée un point P appartenant à une courbe
20 elliptique donnée et un entier d . L'entier d est noté $d=(d(t),d(t-1), \dots, d(0))$, où $(d(t),d(t-1), \dots, d(0))$ est la représentation binaire de d , avec $d(t)$ le bit de poids fort et $d(0)$ le bit de poids faible. L'algorithme retourne en sortie le point $Q=d.P$.

25 L'algorithme « double and add » a deux variantes, selon que l'on commence les calculs par les bits de poids fort ou de poids faible de d .

La première variante comporte les 3 étapes suivantes :

30 1) Initialiser le point Q avec la valeur P

2) Pour i allant de t à 0 exécuter :

2a) Remplacer Q par $2Q$

2b) Si $d(i)=1$ remplacer Q par $Q+P$

3) Retourner Q .

35 La seconde variante comporte les 3 étapes suivantes :

1) Initialiser le point Q avec le point à l'infini O et un accumulateur A avec la valeur P .

2) Pour i allant de 0 à t exécuter :

2a) Si $d(i)=1$ remplacer Q par $Q+A$

2b) Remplacer A par $2A$

3) Retourner Q .

5 Il est apparu que l'implémentation sur carte à puce d'un algorithme de chiffrement à clé publique du type courbe elliptique était vulnérable à des attaques consistant en une analyse différentielle de consommation de courant permettant de retrouver la
10 clé privée de déchiffrement. Ces attaques sont appelées attaques DPA, acronyme pour Differential Power Analysis. Le principe de ces attaques DPA repose sur le fait que la consommation de courant du microprocesseur exécutant des instructions varie
15 selon la donnée manipulée.

En particulier, lorsqu'une instruction manipule une donnée dont un bit particulier est constant, la valeur des autres bits pouvant varier, l'analyse de la consommation de courant liée à l'instruction
20 montre que la consommation moyenne de l'instruction n'est pas la même suivant que le bit particulier prend la valeur 0 ou 1. L'attaque de type DPA permet donc d'obtenir des informations supplémentaires sur les données intermédiaires manipulées par le
25 microprocesseur de la carte lors de l'exécution d'un algorithme cryptographique. Ces informations supplémentaires peuvent dans certain cas permettre de révéler les paramètres privés de l'algorithme de déchiffrement, rendant le système cryptographique non
30 sûr.

Dans la suite de ce document on décrit un procédé d'attaque DPA sur un algorithme de type courbe elliptique réalisant une opération du type multiplication scalaire d'un point P par un entier d ,
35 l'entier d étant la clé secrète. Cette attaque permet de révéler directement la clé secrète d . Elle compromet donc gravement la sécurité de

l'implémentation de courbes elliptiques sur une carte à puce.

La première étape de l'attaque est l'enregistrement de la consommation de courant correspondant à l'exécution de la première variante de l'algorithme « double and add » décrit précédemment pour N points distincts $P(1), \dots, P(N)$. Dans un algorithme à base de courbes elliptiques, le microprocesseur de la carte à puce va effectuer N multiplications scalaires $d.P(1), \dots, d.P(N)$.

Pour la clarté de la description de l'attaque, on commence par décrire une méthode permettant d'obtenir la valeur du bit $d(t-1)$ de la clé secrète d , où $(d(t), d(t-1), \dots, d(0))$ est la représentation binaire de d , avec $d(t)$ le bit de poids fort et $d(0)$ le bit de poids faible. On donne ensuite la description d'un algorithme qui permet de retrouver la valeur de d .

On groupe les points $P(1)$ à $P(N)$ suivant la valeur du dernier bit de l'abscisse de $4.P$, où P désigne un des points $P(1)$ à $P(N)$. Le premier groupe est constitué des points P tels que le dernier bit de l'abscisse de $4.P$ est égal à 1. Le second groupe est constitué des points P tels que le dernier bit de l'abscisse de $4.P$ est égal à 0. On calcule la moyenne des consommations de courant correspondant à chacun des deux groupes, et on calcule la courbe de différence entre ces deux moyennes.

Si le bit $d(t-1)$ de d est égal à 0, alors l'algorithme de multiplication scalaire précédemment décrit calcule et met en mémoire la valeur de $4.P$. Cela signifie que lors de l'exécution de l'algorithme dans une carte à puce, le microprocesseur de la carte va effectivement calculer $4.P$. Dans ce cas, dans le premier groupe de message le dernier bit de la donnée manipulée par le microprocesseur est toujours à 1, et dans le deuxième groupe de message le dernier bit de la donnée manipulée est toujours à 0. La moyenne des consommations de courant correspondant à chaque

groupe est donc différente. Il apparaît donc dans la courbe de différence entre les 2 moyennes un pic de différentiel de consommation de courant.

Si au contraire le bit $d(t-1)$ de d est égal à 1, l'algorithme d'exponentiation décrit précédemment ne calcule pas le point 4.P. Lors de l'exécution de l'algorithme par la carte à puce, le microprocesseur ne manipule donc jamais la donnée 4.P. Il n'apparaît donc pas de pic de différentiel de consommation.

Cette méthode permet donc de déterminer la valeur du bit $d(t-1)$ de d .

L'algorithme décrit dans le paragraphe suivant est une généralisation de l'algorithme précédant. Il permet de déterminer la valeur de la clé secrète d :

On définit l'entrée par N points notés $P(1)$ à $P(N)$ correspondant à N calculs réalisés par la carte à puce et la sortie par un entier h .

Ledit algorithme s'effectue de la manière suivante en trois étapes.

1) Exécuter $h=1$;

2) Pour i allant de $t-1$ à 1, exécuter :

2)1) Classer les points $P(1)$ à $P(N)$ suivant la valeur du dernier bit de l'abscisse de $(4 \cdot h).P$;

2)2) Calculer la moyenne de consommation de courant pour chacun des deux groupes ;

2)3) Calculer la différence entre les 2 moyennes ;

2)4) Si la différence fait apparaître un pic de différentiel de consommation, faire $h=h \cdot 2$;
sinon faire $h=h \cdot 2 + 1$;

3) Retourner h .

L'algorithme précédent fournit un entier h tel que $d=2 \cdot h$ ou $d=2 \cdot h + 1$. Pour obtenir la valeur de d , il suffit ensuite de tester les deux hypothèses possibles. L'attaque de type DPA décrite permet donc de retrouver la clé privée d .

Une attaque équivalente s'applique à la seconde variante de l'algorithme de multiplication scalaire

de type « double and add », et plus généralement à tous les algorithmes de multiplication scalaire sur courbe elliptique.

Le procédé de l'invention consiste en
 5 l'élaboration d'une nouvelle contre-mesure permettant de se prémunir contre l'attaque DPA précédemment décrite.

Ce procédé consiste à « masquer » la clé secrète d par laquelle on veut multiplier un point P de la
 10 courbe elliptique par une valeur aléatoire r de même longueur.

Ledit procédé de contre-mesure de la présente invention dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé publique
 15 basé sur l'utilisation des courbes elliptiques consistant à calculer, à partir de la clé privée d et du nombre de points n de ladite courbe elliptique, un nouvel entier de déchiffrement d' tel que le déchiffrement d'un message quelconque, au moyen d'un
 20 algorithme de déchiffrement, avec d' permet d'obtenir le même résultat qu'avec d, en réalisant l'opération $Q=d.P$, P étant un point de la courbe sur lequel est appliqué l'algorithme de multiplication scalaire, est caractérisé en ce qu'il comprend les étapes
 25 suivantes :

- 1) Tirage d'une valeur aléatoire r de même taille que d;
- 2) Calcul de l'entier d' tel que : $d'=d+r$;
- 3) Opération de multiplication scalaire dont le
 30 résultat est le point Q' de la courbe tel que : $Q'=d'.P$;
- 4) Opération de multiplication scalaire dont le résultat est le point S de la courbe tel que : $S=r.P$;
- 5) Calcul du point Q de la courbe tel que : $Q=Q'-S$.

35 L'avantage de ce procédé par rapport aux trois contre-mesures du brevet français 99.03920 est qu'il permet de prévoir une contre-mesure à la fois différente et mieux adaptée à certains types de

courbes elliptiques. Plus précisément, lorsque l'algorithme de multiplication scalaire s'effectue selon ladite deuxième variante de l'algorithme « double and add », l'opération de doublement du point P est commune au calcul des points $Q' = d'.P$ et $S = r.P$. Le sur-coût en temps de calcul de cette contre-mesure est donc réduit aux opérations d'addition effectuées lors du calcul du point $S = r.P$. Ceci présente un avantage incontestable lorsque l'on utilise des courbes elliptiques pour lesquelles le doublement d'un point est une opération aussi coûteuse en temps de calcul que l'addition de deux points.

Le présent procédé se différencie par rapport aux contre-mesures du brevet français 99.03920 en ce que l'aléa r est un entier qui masque ledit entier de déchiffrement d et non un point aléatoire de la courbe qui masque le point P , et en ce que le calcul du résultat Q comporte une étape de calcul du point $S=r.P$, ce qui n'est pas nécessaire dans ledit brevet français 99.03920 lorsque l'aléa r est un multiple du nombre n de points de la courbe.

Le procédé de contre-mesure de l'invention comprend trois variantes.

La première variante consiste en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement. Lors de la première exécution de l'algorithme de déchiffrement, l'algorithme est exécuté suivant le procédé en cinq étapes décrit précédemment. Tant que le compteur n'a pas atteint la valeur limite T , les étapes 1 et 4 du procédé décrit précédemment ne sont pas exécutées, le point S gardant la valeur prise lors de l'exécution précédente. Lorsque le compteur atteint la valeur limite T , l'algorithme de déchiffrement s'effectue suivant le procédé décrit précédemment en cinq étapes, et le compteur est remis à zéro. Dans la pratique, on peut prendre $T=16$.

La deuxième variante consiste en ce que la carte possède initialement en mémoire un point de la courbe elliptique tel que $S=r.P$. Les étapes 1 et 4 de l'algorithme de déchiffrement précédent sont
5 remplacées par les étapes 1' et 4' suivantes:

1') Remplacer r par $2.r$:

4') Remplacer S par $2.S$.

La troisième variante consiste en une modification de la deuxième variante caractérisée en
10 ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement. Lors de la première exécution de l'algorithme de déchiffrement, l'algorithme est exécuté suivant le procédé en cinq étapes de la deuxième variante décrit
15 précédemment. Tant que le compteur n'a pas atteint une valeur limite T , les étapes 1' et 4' du procédé décrit précédemment ne sont pas exécutées, le point S gardant la valeur prise lors de l'exécution précédente. Lorsque le compteur atteint une valeur
20 limite T , l'algorithme de déchiffrement s'effectue suivant le procédé précédemment décrit en cinq étapes, et le compteur est remis à zéro. Dans la pratique, on peut prendre $T=16$.

L'application de ce procédé de contre-mesure
25 permet de protéger tout l'algorithme cryptographique basé sur les courbes elliptiques contre l'attaque DPA précédemment décrite. La présente contre-mesure complète les trois contre-mesures présentées par le brevet français 99.03920 et peut être combinée avec
30 l'une quelconque de ces trois contre-mesures pour en former une nouvelle. Elle s'applique à tout composant électronique, du type puce électronique pour carte à puce par exemple.

REVENDEICATIONS

- 1- Procédé de contre-mesure dans un composant
 5 électronique mettant en oeuvre un algorithme de cryptographie à clé publique basé sur l'utilisation des courbes elliptiques consistant à calculer, à partir de la clé privée d et du nombre de points n de ladite courbe elliptique, un nouvel entier de déchiffrement d'
 10 tel que le déchiffrement d'un message quelconque, au moyen d'un algorithme de déchiffrement, avec d' permet d'obtenir le même résultat qu'avec d , en réalisant l'opération $Q=d.P$, P étant un point de la courbe sur lequel est appliqué l'algorithme de multiplication
 15 scalaire, procédé caractérisé en ce qu'il comprend les étapes suivantes :
- 1) Tirage d'une valeur aléatoire r de même taille que d ;
 - 2) Calcul de l'entier d' tel que : $d'=d+r$;
 - 20 3) Opération de multiplication scalaire dont le résultat est le point Q' de la courbe tel que : $Q'=d'.P$;
 - 4) Opération de multiplication scalaire dont le résultat est le point S de la courbe tel que : $S=r.P$;
 - 25 5) Calcul du point Q de la courbe tel que : $Q=Q'-S$.
- 2- Procédé de contre-mesure selon la revendication 1 caractérisé en ce qu'un nouvel entier de déchiffrement d' est calculé à chaque nouvelle exécution de
 30 l'algorithme de déchiffrement.
- 3- Procédé de contre-mesure selon la revendication 1 caractérisé en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de déchiffrement jusqu'à une valeur entière T .
- 35 4- Procédé de contre-mesure selon la revendication 3 caractérisé en ce qu'une fois la valeur T atteinte, un

nouvel entier de déchiffrement d' est calculé selon le procédé de la revendication 1, le compteur étant remis à zéro et le point $S=r.P$ étant stocké en mémoire.

5 5- Procédé de contre-mesure selon la revendication 3 ou la revendication 4 caractérisé en ce que la valeur T est égale à seize.

6- Procédé de contre-mesure selon la revendication 1 caractérisé en ce que la courbe elliptique possède en mémoire un point S , tel que $S=r.P$, les étapes 1 et 4
10 étant alors remplacées par les étapes 1' et 4':

1') Remplacer r par $2.r$:

4') Remplacer S par $2.S$.

7- Procédé de contre-mesure selon la revendication 6 caractérisé en ce qu'un nouvel entier de déchiffrement
15 d' est calculé à chaque nouvelle exécution de l'algorithme de déchiffrement.

8- Procédé de contre-mesure selon la revendication 6 caractérisé en ce qu'un compteur est incrémenté à chaque nouvelle exécution de l'algorithme de
20 déchiffrement jusqu'à une valeur T .

9- Procédé de contre-mesure selon la revendication 8 caractérisé en ce qu'une fois la valeur T atteinte, un nouvel entier de déchiffrement d' est calculé selon le procédé de la revendication 6, et le compteur est remis
25 à zéro.

10- Procédé de contre-mesure selon la revendication 8 ou la revendication 9 caractérisé en ce que la valeur T est égale à seize.

11- Composant électronique mettant en oeuvre le procédé
30 selon l'une quelconque des revendications 1 à 10.

09/774,674

THIS PAGE BLANK (USPTO)